

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平5-53921

(43) 公開日 平成5年(1993)3月5日

| (51) Int.Cl. ⁵ | 識別記号 | 片内整理番号 | F I | 技術表示箇所 |
|---------------------------|---------|---------|-----|--------|
| G 0 6 F 12/14 | 3 2 0 B | 9293-5B | | |
| 15/78 | 5 1 0 Z | 7530-5L | | |
| G 0 9 C 1/00 | | 7922-5L | | |

審査請求 未請求 請求項の数3(全 7 頁)

(21) 出願番号 特願平3-237147

(22) 出願日 平成3年(1991)8月23日

(71) 出願人 000006655

新日本製鐵株式会社

東京都千代田区大手町2丁目5番3号

(72) 発明者 佐々木 誠

東京都千代田区大手町2-6-3 新日本
製鐵株式会社内

(72) 発明者 柴田 高幸

東京都千代田区大手町2-6-3 新日本
製鐵株式会社内

(72) 発明者 成田 喜則

東京都千代田区大手町2-6-3 新日本
製鐵株式会社内

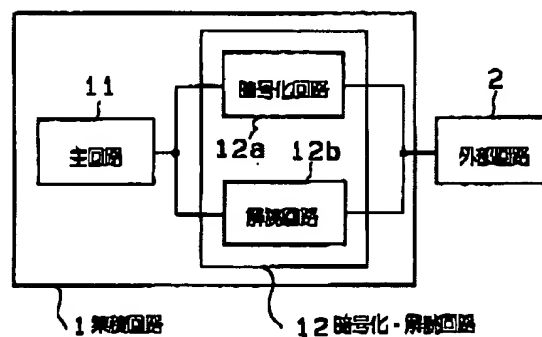
(74) 代理人 弁理士 國分 孝悦

(54) 【発明の名称】 集積回路

(57) 【要約】

【目的】 外部回路と接続されてデータの入出力を行う集積回路において、データの複製および回路の機能の複製を防止する。

【構成】 集積回路1に、主たる機能を実現する主回路11、暗号化解読回路12を設けた。暗号化解読回路12は、主回路11から出力されたデータを暗号化し外部回路2へ出力する暗号化回路12aと外部回路2から入力された暗号化されたデータを解読し主回路11へ出力する解読回路12bを有している。集積回路1に入出力されるデータを複製しても主回路11の機能のみを複製した回路では使用できない。また、データが暗号化されているため、主回路の複製も困難である。



(2)

特開平5-53921

1

【特許請求の範囲】

【請求項1】 外部装置との間でデータの入出力が行われ、該入出力されるデータ処理する集積回路において、該集積回路は、

前記集積回路の機能に基づく種々の動作を行う主回路手段と、

前記入出力されるデータを暗号化または解読する暗号処理手段とを有し、

前記外部装置との間で暗号化されたデータの入出力が行われることを特徴とする集積回路。

【請求項2】 外部装置との間でデータの入出力が行われ、該入出力されるデータ処理する集積回路において、該集積回路は、

前記集積回路の機能に基づく種々の動作を行う主回路手段と、

前記主回路手段から出力されるデータを暗号化する暗号化手段と、前記外部装置から入力される暗号化されたデータを解読する解読手段とからなる暗号処理手段とを有し、

前記外部装置との間で暗号化されたデータの入出力が行われることを特徴とする集積回路。

【請求項3】 前記主回路手段がCPUであり、前記集積回路は1チップに形成された1チップマイクロコンピュータであることを特徴とする請求項2に記載の集積回路。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、外部装置に接続されてデータの入出力を行う集積回路に関し、授受されるデータの複製および集積回路の機能の複製を防止できる集積回路に関する。

【0002】

【従来の技術】 従来、接続される回路すなわち外部装置とデータの入出力を行う集積回路は、入出力されるデータの複製を防止するために、システムを構成する集積回路以外のハードウェアを利用した複製防止データをデータの一部として組み込み、これにより、データの複製を困難にしていた。

【0003】

【発明が解決しようとする課題】 しかし、従来の集積回路に接続された回路とデータの入出力を行う集積回路においては、複製防止データを組み込んだデータを用いる場合であっても、集積回路が突動作しているとき、集積回路に入出力するデータをサンプルすることにより、データの部分的な複製が可能であり、これを防止することはできないという問題があった。

【0004】 本発明は、このような問題を解消し、プログラムまたはデータの複製防止機能を有する集積回路を提供することを目的とする。

【0005】

2

【課題を解決するための手段】 本発明の集積回路は、上記課題を解決するために、集積回路の機能に基づく種々の動作を行う主回路手段と、入出力されるデータを暗号化または解読する暗号処理手段とを有する。

【0006】

【作用】 本発明によれば、入出力されるデータを暗号化または解読する暗号処理手段を具備しているから、主回路手段から出力されるデータを暗号化して外部装置へ出力するか、または外部装置から入力される暗号化されたデータを解読して主回路手段へ出力することができる。そして、集積回路と外部装置との間で入出力されるデータは暗号化されたデータであるから、入出力されるデータを複製しても、解読手段がなければこのデータを利用することができない。したがって、主回路の機能のみを複製した回路ではこのデータを使用することができない。また、データが暗号化されているため、主回路の複製も困難である。

【0007】

【実施例】 次に図面を用いて本発明の実施例を説明する。図1に、本発明による集積回路の一実施例を示す。図1は、集積回路と外部回路とが接続された状態を示す。集積回路1は主回路11および暗号化・解読回路12を備えている。主回路11は、集積回路1の主な機能を実現するものであり、集積回路1の機能に基づく種々の動作を行う。主回路11は、たとえばCPUによって構成される。

【0008】 暗号化・解読回路12は、データの暗号化および暗号化されたデータの解読の機能を有する回路であり、同図に示すように暗号化回路12aと解読回路12bとにより構成されている。暗号化回路12aは主回路11から入力されるデータを暗号化して外部回路2へ出力し、解読回路12bは外部回路2から入力されるデータを解読して主回路11へ出力する。

【0009】 暗号化の方式としては種々のものを用いることが可能であるが、本実施例においてはUSAスタンダード暗号化方式(DES)をベースとしたアルゴリズムにより暗号化を行う。

【0010】 DESは、0と1からなる2元データに対するブロック暗号であり、2元データを64ビットのブロックに分割し、各ブロックについて転置と換字を繰り返すことにより暗号化を行うものである。この場合に転置はあらかじめ固定された変換であるが、換字には64ビットのキーが使用され、このキーによって換字が制御される。一方、復号すなわち解読においては、暗号化とは逆に換字および転置が繰り返される。

【0011】 暗号化・解読回路12には外部回路2が接続されている。外部回路2は集積回路1との間でデータを授受する外部装置であり、たとえば集積回路1から出力されるデータを記憶する記憶装置、または集積回路1によって処理されるデータを読み出す記憶装置である。

(3)

特開平5-53921

なお、図示しないが、データの入出力を制御するインタフェース制御回路たる入出力回路を暗号化・解読回路12に接続し、この入出力回路を通して外部回路2とのデータの授受を行うようにしてもよい。

【0012】この装置によれば、集積回路1が外部回路2にデータを出力する場合、主回路11により処理され出力されたデータは暗号化・解読回路12に入力され、暗号化回路12aにより暗号化される。暗号化回路12aに入力されたデータは前述のような暗号化によって暗号化されたデータに変換される。暗号化されたデータは、外部回路2へ出力される。

【0013】一方、外部回路2から集積回路1へデータが入力される場合には、外部回路2から入力される暗号化されたデータは暗号化・解読回路12の解読回路12bで解読された後、主回路11に供給され所定の処理が行われる。

【0014】このように暗号化・解読回路12により暗号化されたデータが外部装置2へ出力され、また、外部装置2からは暗号化されたデータが入力された暗号化・解読回路12により解読される。したがって、外部装置2との間で入出力されるデータは暗号化されたデータであるから、集積回路1に入出力されるデータを複製しても解読手段を持たない限り、複製したデータを利用することができず、主回路11の機能のみを複製した回路ではこのデータを使用することができない。また、データが暗号化されているため、主回路11の複製も困難である。

【0015】図2には、外部回路2として記憶装置21を接続した場合の例が示されている。記憶装置21は、集積回路1によって処理され、出力されたデータを記憶する記憶装置であり、集積回路1から出力される暗号化されたデータが格納される。この場合には、図1の暗号化・解読回路12の機能は暗号化機能のみで十分であるから、暗号化回路12aに置き換えられている。

【0016】このように接続された装置において、第三者が記憶装置21に格納されたデータを複製した場合にも、複製データを得た者はこのデータを解読する手段を持たない限り、このデータを利用することができない。したがって、集積回路1は複製から保護される。

【0017】図3には、外部回路2として読み出し専用の記憶装置22が使用された場合の例が示されている。この場合には記憶装置22にあらかじめ格納された暗号化されたデータが集積回路1へ読み出され、処理される。この場合には、図1の暗号化・解読回路12の機能は解読機能のみで十分であるから、解読回路12bに置き換えられている。記憶装置22に格納されるデータは主回路11が必要とするデータをあらかじめ暗号化したデータである。この暗号化はたとえば前述のDESによって行われる。図6に示すように、主回路11が必要とする主回路データを供給し（ステップ31）、このデータ

をブロックに分割し（ステップ32）、転送および換字を所定の回数繰り返して暗号化を行い（ステップ33）、暗号化されたデータを得て記憶装置22に格納する（ステップ34）。

【0018】図4には、本発明による集積回路が2個接続された場合の例が示されている。集積回路41は、主回路411および暗号化・解読回路412を有し、暗号化・解読回路412は暗号化回路412aおよび解読回路412bを含んでいる。同様に、集積回路42は主回路421および暗号化・解読回路422を有し、暗号化・解読回路422は暗号化回路422aおよび解読回路422bを含んでいる。暗号化回路412aは解読回路422bに接続され、暗号化回路422aは解読回路412bに接続されている。

【0019】この装置によれば、集積回路41の主回路411から出力されたデータは暗号化回路412aで暗号化され、集積回路42の解読回路422bで解読された後、主回路421へ送られる。また、集積回路42の主回路421から出力されたデータは暗号化回路422aで暗号化され、集積回路41の解読回路412bで解読された後、主回路411へ送られる。

【0020】集積回路41の主回路411と集積回路42の主回路421の主回路としての機能は通常異なるものである。また、集積回路41の行う暗号化と集積回路42の行う暗号化のアルゴリズムは同じものである必要はないが、暗号化回路412aが生成する暗号を解読回路422bが解読でき、かつ、暗号化回路422aが生成する暗号を解読回路412bが解読できるようにされている。集積回路41と集積回路42の暗号化アルゴリズムが異なる場合には、データ複製防止機能はさらに向上する。

【0021】図5には、本発明による集積回路がワンチップマイクロコンピュータ6および入出力用集積回路63として用いられ、これらが互いに接続されるとともに、メモリ64に接続された場合の一例が示されている。ワンチップマイクロコンピュータ6はCPU61、暗号化・解読回路62aおよび暗号化・解読回路62bを有しており、CPU61が図1の主回路11に相当する。入出力用集積回路63は、暗号化・解読回路631および入出力回路632を有し、入出力回路632が図1の主回路11に相当する。

【0022】ワンチップマイクロコンピュータ6の暗号化・解読回路62aは、入出力用集積回路63の暗号化・解読回路631と接続され、暗号化・解読回路62bはメモリ64と接続されている。入出力用集積回路63の入出力回路632は入出力端子65を介して外部装置と接続されている。

【0023】ワンチップマイクロコンピュータ6に接続されたメモリ64には、CPU61のプログラムとデータが暗号化されたデータとして格納されている。メモリ

(4)

特開平5-53921

5

64から読み出されたプログラムおよびデータは暗号化・解読回路62bにおいて解読され、CPU61に送られる。CPU61はこのプログラムおよびデータにより所定の処理を行う。

【0024】また、CPU61からのデータは暗号化・解読回路62aにおいて暗号化されて入出力用集積回路63の暗号化・解読回路631に送られ、暗号化・解読回路631で解読された後、入出力回路632に送られる。そして入出力回路632で入出力処理を行われた後、入出力端子65を通して外部装置へ出力される。逆に、外部装置から入出力端子65を通して入力されたデータは、入出力回路632で入出力処理を行われた後、暗号化・解読回路631に送られて暗号化され、ワンチップマイクロコンピュータ6の暗号化・解読回路62aへ出力される。データは暗号化・解読回路62aで解読され、CPU61に送られる。CPU61で処理されたデータは暗号化・解読回路62bにおいて暗号化され、メモリ64に記憶される。

【0025】本装置においても、前述のような暗号化アルゴリズムによって暗号化されたデータがワンチップマイクロコンピュータ6、入出力用集積回路63およびメモリ64の間で入出力される。

【0026】一般に乱数を用いた暗号化や暗号化鍵によるビット反転とビット入れ換え操作を多数行う暗号化では、暗号化アルゴリズムを知らずに暗号化されたデータやプログラムを解読することは、非常に困難である。また、集積回路のマスクパターンから暗号化アルゴリズムを解析するか、あるいは、CPU61と暗号化・解読回路62a、62bの間の信号を解析することが非常に困難であることは言うまでもない。

【0027】図5の実施例においては、メモリ64に格納されたデータまたはプログラムを複製しても、このデータを解読しないかぎり利用できないため、CPU61のデータまたはプログラムを保護することができる。また、入出力用集積回路63に対するコマンドやデータが暗号化されていることにより、入出力集積回路63のコマンド体系やデータ形式が保護されるため、入出力集積回路63の複製を防止できる。

【0028】

【発明の効果】以上説明したように本発明によれば、集

6

積回路には暗号化されたデータが入出力されるから、入出力されるデータを複製しても、主回路の機能のみを複製した回路ではこのデータを使用することができない。暗号化されたデータを解読するには暗号化アルゴリズムを調査しデータを解読するか、または、集積回路の内部で主回路と暗号化・解読回路の間の信号を直接サンプリングしなければならないため、データの複製は非常に困難である。また、データを暗号化しているため主回路の複製も困難であるから、回路を複製から有効に保護することができる。

【図面の簡単な説明】

【図1】本発明による集積回路の一実施例を示すブロック図である。

【図2】本発明による集積回路を記憶装置に接続した実施例を示すブロック図である。

【図3】本発明による集積回路を読み出し専用記憶装置に接続した実施例を示すブロック図である。

【図4】本発明による集積回路を2個接続した実施例を示すブロック図である。

【図5】本発明による集積回路をワンチップマイクロコンピュータおよび入出力用集積回路として用いた実施例を示すブロック図である。

【図6】暗号化データを作成する手順を示すフロー図である。

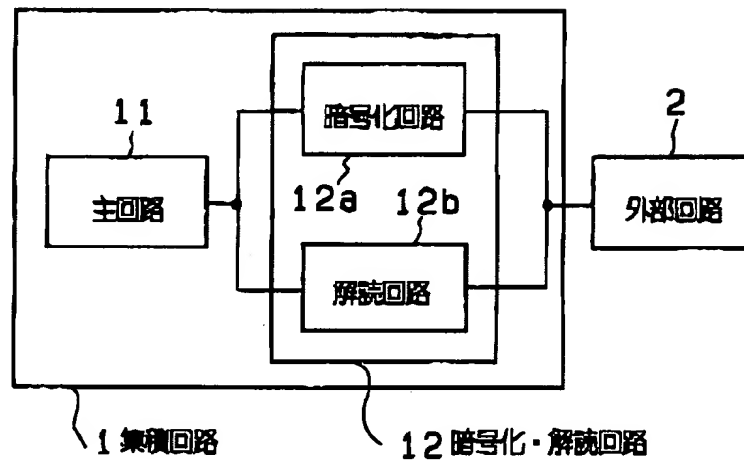
【符号の説明】

- 1 集積回路
- 2 外部回路
- 6 ワンチップマイクロコンピュータ
- 12 暗号化・解読回路
- 21 記憶装置
- 22 記憶装置
- 41 集積回路
- 42 集積回路
- 61 CPU
- 62a 暗号化・解読回路
- 62b 暗号化・解読回路
- 63 入出力集積回路
- 64 メモリ
- 65 入出力端子

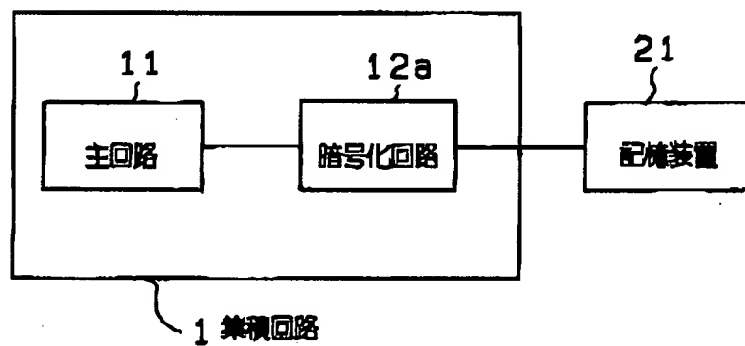
(5)

特開平5-53921

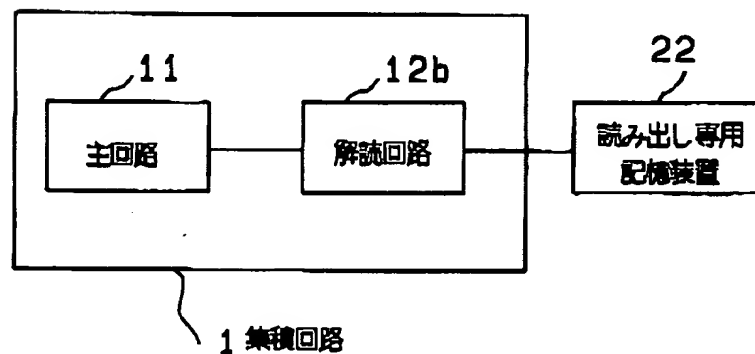
【図1】



【図2】



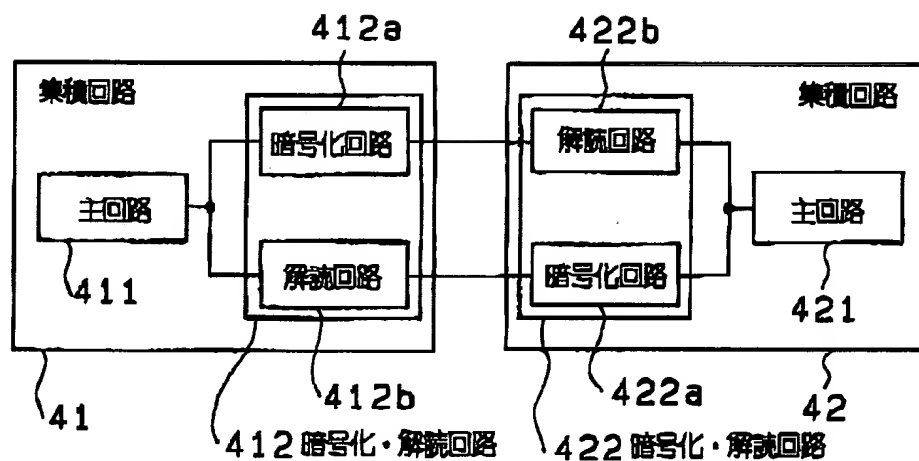
【図3】



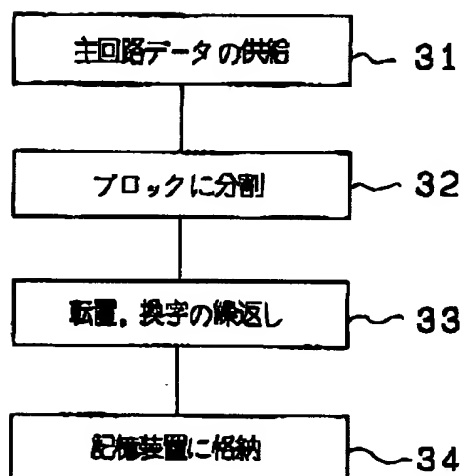
(6)

特開平5-53921

【図4】



【図6】



(7)

特開平5-53921

【図5】

